28 JUL 2004

BUNDESREPUBLIK DEUTSCHLAND

EP04/8456

Prioritätsbescheinigung über die Einreichung einer Gebrauchsmusteranmeldung

Aktenzeichen: 203 13 562.8

Anmeldetag: 29. August 2003

Anmelder/Inhaber: Siemens Aktiengesellschaft, 80333 München/DE

Bezeichnung: HMI System zur Bedienung und Beobachtung einer technischen Anlage mit einem mobilen Bedien- und Beobachtungsgerät und gesicherter Datenübertragung

IPC: H 04 L 12/24

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Gebrauchsmusteranmeldung.

München, den 31. März 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Kahle

A 9161
03/00
EDV-L

Beschreibung

HMI System zur Bedienung und Beobachtung einer technischen Anlage mit einem mobilen Bedien- und Beobachtungsgerät und gesicherter Datenübertragung

Die Erfindung betrifft ein HMI System mit zumindest einem mobilen Bedien- und Beobachtungsgerät für die Automatisierungskomponenten einer technischen Anlage.

Technische Anlagen sind alle Arten von technischen Geräten und Systemen sowohl in Einzelanordnung als auch in datentechnischer Vernetzung z.B. über einen Feldbus. Bei industriellen Anwendungen fallen darunter einzelne Betriebsmittel, z.B. Antriebe; Bearbeitungsmaschinen. Eine technische Anlage kann aber auch eine Produktionsanlage sein, bei der mit lokal verteilten Betriebsmitteln ein gesamter technischer Prozess betrieben wird, z.B. eine chemische Anlage oder Fertigungsstraße. Technische Anlagen werden mit speziellen digitalen Datenverarbeitungssystemen, auch Automatisierungskomponenten genannt, gesteuert und bedient. In einem solchen System sind einerseits zur direkten Steuerung der technischen Anlage dienende Komponenten vorhanden, d.h. speicherprogrammierbare Steuerungen SPS, auch als „PLC - Programmable Logic Controller" bezeichnet. Zur Entlastung dieser Steuerungen weisen Automatisierungen weitere spezielle Geräte auf, welche eine Schnittstelle für Bedienpersonal bilden. Diese werden als Geräte zum „Bedienen- und Beobachten", abgekürzt „B+B", oder als HMI Geräte, d.h. Human Machine Interface, bezeichnet.

Der Begriff HMI Gerät ist ein Oberbegriff und umfasst alle zu dieser Gruppe von Geräten gehörigen Komponenten. Als ein Beispiel sollen „Operator Panels", auch als „Bedienpanels" bzw. kurz als „OP" bezeichnet, genannt werden. Diese können stationär oder mobil ausgeführt sein. HMI Geräte dienen in einer vernetzten Automatisierung als Hilfsmittel für Bedienpersonal, um Prozessdaten der zu steuernden technischen Anlage an-

zeigen und bedienen zu können. Diese Funktion wird mit „Supervisor Control and Data Akquisition" (SCADA) bezeichnet. Hierzu ist das HMI Gerät in der Regel hardwaremäßig speziell aufgebaut, d.h. es verfügt z.B. über einen Touchscreen und ist gegen Umwelteinflüsse besonders abgeschirmt. Weiterhin wird darin eine spezielle Software ausgeführt. Diese stellt Funktionen bereit, womit Komfort, Qualität und Sicherheit einer Bedienung durch eine Bedienperson verbessert. So können über HMI Geräte z.B. interaktive Prozessabbilder der zu bedienenden technischen Anlage visualisiert, bedient, projektiert und generiert werden. Hiermit ist einerseits eine selektive Anzeige von Reaktionen der technischen Anlage möglich, meist in Form von Messwerten und Meldungen. Andererseits wird es durch gezielte Vorgabe von Bedienhandlungen und Dateneingaben ermöglicht, die technische Anlage in gewünschte Zustände zu überführen.

Vielfach sind die HMI Geräte z.B. in Form von Terminals oder Operator Panels als stationäre Komponenten in ein Automatisierungssystem fest integriert. Dabei sind die Komponenten vielfach über einen Feldbus verbunden, der insbesondere bezüglich Ausfall- und Übertragungssicherheit die bei industriellen Anwendungen notwendigen Anforderungen erfüllt. Derartige Netzwerke stellen in der Automatisierungstechnik ein geschlossenes System dar und sind auf Grund dieser Eigenschaft sicher gegenüber Fremdzugriffen. Falls dennoch in Anwendungsfällen eine Öffnung eines Automatisierungssystems insbesondere durch Anbindung an das Internet erfolgt, um z.B. Prozess-, Bedien- und Beobachtungsdaten zwischen einem lokalen Automatisierungssystem und einer sogenannten „Remote Location" über das Internet auszutauschen, so kann ein derartiger Anschlusspunkt mit bekannten Maßnahmen, wie z.B. der Installation einer Firewall, gegenüber Fremdzugriffen abgesichert werden.

Anders ist die Situation, wenn die HMI Geräte nicht ausschließlich stationär, sondern auch in Form von mobilen Ope-

rator Panels ausgeführt sind. Ein derartiges Automatisierungssystem, dessen Feldbus um mindestens eine Funkstrecke zu einem mobilen Bedien- und Beobachtungsgerät erweitert ist, kann zwar logisch weiterhin als geschlossen angesehen werden. Dennoch stellt die Funkstrecke einen Bereich dar, der besonders gefährdet ist gegenüber beabsichtigten und zufälligen Fremdeingriffen. Diese können in Automatisierungssystemen Wirkungen hervorrufen, die über die bekannten Auswirkungen z.B. von Virenangriffen auf private und kommerzielle Computer und Computernetzwerke hin ausgehen. So sind in einem solchen Falle nicht nur wirtschaftliche Einbußen verursacht durch einen Ausfall des Automatisierungssystems und einer von abhängigen Fertigungsanlage zu befürchten. Vielmehr ist es nicht ausgeschlossen, dass die Sicherheit von Personen in einer Fertigungsanlage in Frage gestellt wird, wenn Fremdeingriffe auf eine Funkstrecke zwischen einem mobilen Bedien- und Beobachtungsgerät und den weiteren Komponenten einer Automatisierungsanlage ausgeübt werden.

Der Erfindung liegt somit die Aufgabe zu Grunde, ein HMI System so weiter zu gestalten, dass auch mobile Bedien- und Beobachtungsgeräte in einer gegenüber Fremdeingriffen sicheren Weise in ein Automatisierungssystem eingebunden sind.

Das erfindungsgemäße HMI System mit zumindest einem mobilen Bedien- und Beobachtungsgerät für die Automatisierungskomponenten einer technischen Anlage weist eine Funkstrecke zur berührungslosen Datenübertragung zwischen dem mobilen Bedien- und Beobachtungsgerät und den Automatisierungskomponenten auf. Zur Sicherung der Datenübertragung von den Automatisierungskomponenten zum mobilen Bedien- und Beobachtungsgerät ist eine erste Firewall und zur Sicherung der Datenübertragung vom mobilen Bedien- und Beobachtungsgerät zu den Automatisierungskomponenten eine zweite Firewall vorhanden.

Die Erfindung hat den Vorteil, dass unter Einsatz von Firewalls, d.h. bei der Sicherung der Entgegennahme von Daten ü-

ber kabelgebundene Kommunikationsstrecken erprobten Mitteln, eine Absicherung auch des bidirektionalen Datenverkehrs auf einer Funkstrecke zwischen einem mobilen Bedien- und Beobachtungsgerät und den weiteren Komponenten der Automatisierung einer technischen Anlage erfolgen kann.

Vorteilhaft ist die zweite Firewall in eine Automatisierungskomponente integriert. Hierdurch kann ein zusätzlicher Hardware Aufwand vermieden werden. Weisen die Automatisierungskomponenten eine Funkschnittstelle, auch Funk Access Point genannt, zur Ankopplung an die Funkstrecke auf, so ist eine Integration der zweiten Firewall in diese Funkschnittstelle besonders vorteilhaft. Hierdurch ist eine besonders gute Absicherung aller dahinter liegenden Automatisierungskomponenten besonders dann möglich, wenn diese gemeinsam mit der Funkschnittstelle über einen Feldbus miteinander verkoppelt sind.

Weiterhin ist die erste Firewall vorteilhaft unmittelbar in das mobile Bedien- und Beobachtungsgerät integriert. Hierdurch können Manipulationen insbesondere bei einer gekapselten Ausführung des Gehäuses des mobilen Bedien- und Beobachtungsgeräts erschwert werden.

Schließlich kann die Datenübertragungssicherheit des erfindungsgemäßen HMI Systems weiter dadurch erhöht werden, dass die Automatisierungskomponenten einen Radius-Server aufweisen, der vorteilhaft ebenfalls als singuläre Komponente an den Feldbus angeschlossen ist. Zusätzlich zu den Filtermechanismen der Firewalls bietet der Radius Server einen sogenannten „Remote Authentification Dial-In Service". Es ist somit eine Authentifizierung der Benutzer des mobilen Bedien- und Beobachtungsgeräts, also eine gesicherte Benutzerverwaltung, möglich.

Die Erfindung wird anhand von einem, in der Figur 1 dargestellten Ausführungsbeispiel nachfolgend näher erläutert.

Die technische Anlage TA in Fig. 1 verfügt über technische Betriebsmittel M, die z.B. Bestandteil einer fertigungs- oder prozesstechnischen Anlage sein können. Zu deren Steuerung sind Automatisierungskomponenten S vorhanden, die über einen Feldbus FB auf die technischen Betriebsmittel M insbesondere durch Vermittlung von Messwertgebern, Stellungsreglern und verschiedenen anderen sogenannten „Process Instruments" eingreifen.

Die Automatisierungskomponenten S in FIG 1 verfügen beispielhaft über ein Automatisierungsgerät AS, z.B. eine speicherprogrammierbare Steuerung SPS, welche die Steuerung der technischen Betriebsmittel M gegebenenfalls in Echtzeit bewirkt. Zur Bedienung- und Beobachtung der Steuerung, der technischen Betriebsmittel M und z.B. von ablaufenden Steuerungs-, Diagnose, Alarmverarbeitungs- und Langzeitbeobachtungsprozessen ist ein stationäres Bedien- und Beobachtungsgerät SP vorhanden, dass z.B. als ein Operator Panel mit Touch Screen und Mitteln zum Fronteinbau in einen Schaltschrank ausgeführt sein kann. Das stationäre Bedien- und Beobachtungsgerät SP verfügt z.B. über ein Display SBD und eine Tastatur SBT. Es ist wie die anderen Automatisierungskomponenten an einen Feldbus FB angeschlossen.

Zusätzlich zum stationären Bedien- und Beobachtungsgerät SP verfügt das in FIG 1 dargestellte HMI System über zumindest ein mobiles Bedien- und Beobachtungsgerät MP, z.B. ein kabelloses Hand-Held Terminal. Auch dieses verfügt z.B. über ein Display MPD und eine Tastatur MPT. Weiterhin können Not-Aus- und Quittungstaste und z.B. Schlüsselschalter vorgesehen sein.

Das mobile Bedien- und Beobachtungsgerät MP tauscht in einer berührungslosen Weise Daten über eine Funkstrecke FS mit den Automatisierungskomponenten S der technische Anlage TA aus. Dabei ist die Funkstrecke FS bidirektional ausgeführt. Ein erster Datenstrom in einer von den Automatisierungskomponen-

ten S zu dem Bedien- und Beobachtungsgerät MP verlaufenden Übertragungsrichtung FAF übermittelt bevorzugt Anzeigen, Alarme, Meldungen, Messwerte und vieles mehr, um einen Benutzer insbesondere über den Zustand der technischen Anlage TA in Kenntnis zu setzen. Ein zweiter Datenstrom in einer vom Bedien- und Beobachtungsgerät MP zu den Automatisierungskomponenten S verlaufenden Übertragungsrichtung MPF übermittelt insbesondere Quittierungen, Befehle und vieles mehr, um insbesondere den Zustand der technischen Anlage TA in einer vom Benutzer des mobilen Bedien- und Beobachtungsgeräts MP gewünschten Weise zu verändern.

Erfindungsgemäß ist die bidirektionale Datenübertragung auf der Funkstrecke FS durch ein Paar von vorzugsweise ausführungsgleichen Firewalls MPW und FAW abgesichert, wobei die erste Firewall MPW die Datenübertragung des ersten Datenstromes in Richtung FAF und die zweite Firewall FAW die Datenübertragung des zweiten Datenstromes in Richtung MPF absichert. Die in den Firewalls MPW und FAW geladenen und aktiven Sicherungsprozeduren sind vorteilhaft übereinstimmend bzw. zumindest gleichwirkend.

Vorteilhaft ist die erste Firewall MPW direkt in das mobile Bedien- und Beobachtungsgerät MP integriert. Entsprechend ist die zweite Firewall FAW vorteilhaft in eine Automatisierungskomponente S integriert. Bei der in FIG 1 dargestellten, bevorzugten Ausführung der Erfindung ist die zweite Firewall FAW direkt in eine an den Feldbus FB angeschlossene Funkschnittstelle FA integriert, welche die Automatisierungskomponenten S an die Funkstrecke FS ankoppelt.

Gemäß einer weiteren, in FIG 1 bereits dargestellten Ausführung weisen die Automatisierungskomponenten S einen zusätzlichen RADIUS Server RS auf, der vorteilhaft ebenfalls an den Feldbus FB angeschlossen ist. Dieser stellt einen zusätzlichen, „Remote Authentification Dail-In User" genannten Service zur Verfügung. Hierüber kann die Berechtigung eines Benut-

zers des mobile Bedien- und Beobachtungsgeräts MP überprüft werden.

Das in FIG 1 beispielhaft dargestellte, erfindungsgemäße HMI System weist somit trotz einer an sich sicherheitsgefährdeten Funkschnittstelle zu einem mobilen Bedien- und Beobachtungsgerät MP eine hervorragende Absicherung gegenüber Fremdzugriffen auf. Diese kann durch zusätzliche Maßnahmen, wie z.B. die Einbindung eines Radius Servers noch weiter verbessert werden.

Schutzansprüche

1. HMI System mit zumindest einem mobilen Bedien- und Beobachtungsgerät (MP) für die Automatisierungskomponenten (S) einer technischen Anlage (TA), mit

a) einer Funkstrecke (FS;FAF,MPF) zur berührungslosen Datenübertragung (MPF,FAF) zwischen dem mobilen Bedien- und Beobachtungsgerät (MP) und den Automatisierungskomponenten (S), und mit

b) einer ersten Firewall (MPW) zur Sicherung der Datenübertragung (FAF) von den Automatisierungskomponenten (S) zum mobilen Bedien- und Beobachtungsgerät (MP) und einer zweiten Firewall (FAW) zur Sicherung der Datenübertragung (MPF) vom mobilen Bedien- und Beobachtungsgerät (MP) zu den Automatisierungskomponenten (S).

2. HMI System nach Anspruch 1, wobei die Sicherungsprozeduren in der ersten und zweiten Firewall (MPW,FAW) übereinstimmend bzw. zumindest gleichwirkend sind.

3. HMI System nach einem der Anspruch 1 oder 2, wobei die erste Firewall (MPW) in das mobile Bedien- und Beobachtungsgerät (MP) integriert ist.

4. HMI System nach Anspruch 3, wobei das mobile Bedien- und Beobachtungsgerät (MP) gekapselt ist.

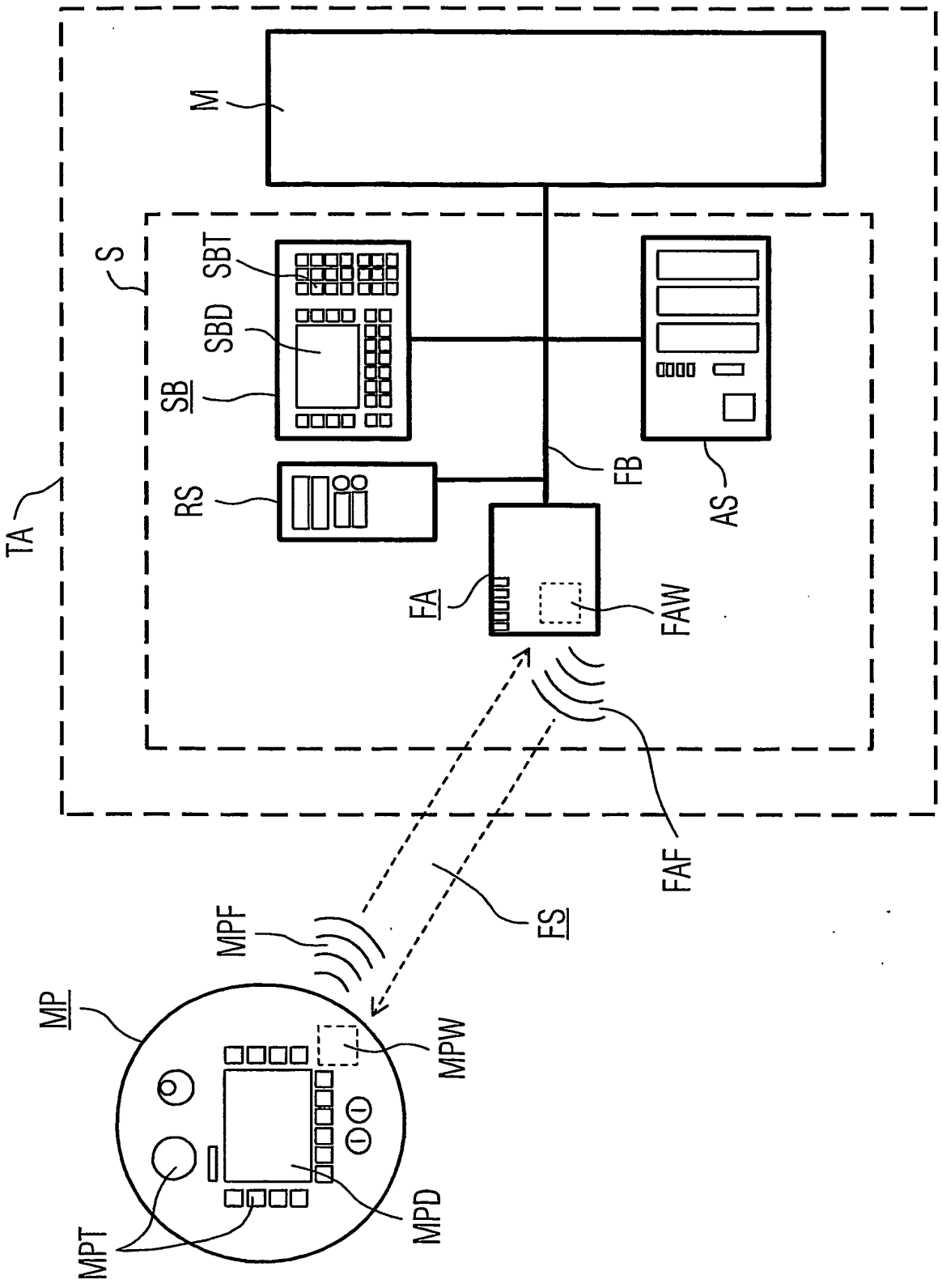
5. HMI System nach einem der vorangegangenen Ansprüche, wobei die zweite Firewall (FAW) in eine Automatisierungskomponente (S) integriert ist.

6. HMI System nach Anspruch 5, wobei die Automatisierungskomponenten (S) zur Ankopplung an die Funkstrecke (FS) eine Funkschnittstelle (FA) aufweisen, in welche die zweite Firewall (FAW) integriert ist.

7. HMI System nach Anspruch 6, wobei die Automatisierungskomponenten (S) einen Feldbus (FB) aufweisen, an den die Funkschnittstelle (FA) angeschlossen ist.

8. HMI System nach einem der vorangegangenen Ansprüche, wobei die Automatisierungskomponenten (S) einen Radius-Server (RS) aufweisen.

9. HMI System nach Anspruch 7, wobei die Automatisierungskomponenten (S) einen Radius-Server (RS) aufweisen, welcher an den Feldbus (FB) angeschlossen ist.


M
S
SBT
SBD
SB
RS
FB
AS
TA
FA
FAW
FAF
FS
MPF
MP
MPW
MPD
MPT